CAMADA DE INTERNET

GABRIEL LUCIOS ANANIAS SORDI

JARAGUÁ DO SUL, SANTA CATARINA, BRASIL

CENTRO UNIVERSITÁRIO CATÓLICA DE SANTA CATARINA

ENGENHARIA DE SOFTWARE

2024

SUMÁRIO

Introdução ................................................................. 1

Protocolos da Camada de Internet .......................................... 2

2.1 Protocolo IP ................................................................... 2

2.2 Protocolo ICMP ................................................................ 3

2.3 Protocolo ARP .................................................................. 4

2.4 Protocolo RARP ............................................................. 5

Funcionamento do Endereçamento IP .................................. 6

3.1 Estrutura do Endereço IP ............................................... 6

3.2 Classes de Endereços IPv4 .............................................. 7

3.3 Máscara de Sub-rede ...................................................... 8

3.4 Fragmentação de Pacotes ............................................... 9

Impactos no Desempenho da Rede ...................................... 10

Segurança na Camada de Internet ..................................... 11

5.1 Vulnerabilidades na Camada de Internet .......................... 11

5.2 Estratégias de Segurança ............................................ 12

Exemplos Práticos ............................................................ 13

6.1 Ping ............................................................................... 13

6.2 Tracert .......................................................................... 14

Referências ............................................................... 15

1. INTRODUÇÃO

A camada de internet é uma das principais do modelo TCP/IP, sendo equivalente à camada de rede do modelo OSI. Ela é responsável por fornecer endereçamento e capacidade de roteamento, permitindo a comunicação entre dispositivos em redes interconectadas. Utiliza protocolos específicos, sendo o principal o protocolo de internet (IP), que define como os pacotes de dados são estruturados, endereçados, transmitidos, roteados e recebidos.

Essa camada desempenha um papel crucial na manutenção de conexões entre redes heterogêneas — ou seja, redes compostas por diferentes tecnologias de acesso, como Wi-Fi, 3G, 4G e 5G. Ela garante a entrega dos pacotes de dados ao destino correto, independentemente da localização física dos dispositivos envolvidos. Para isso, fornece um esquema de endereçamento lógico único (como os endereços IP), permitindo que cada dispositivo conectado à rede seja identificado de forma inequívoca. Além disso, determina o melhor caminho para os pacotes trafegarem entre dispositivos localizados em redes diferentes, utilizando algoritmos e tabelas de roteamento.

A camada de internet opera com comunicação sem conexão, característica do protocolo IP, que envia pacotes independentemente, sem estabelecer uma conexão prévia. Um exemplo importante dessa funcionalidade é o campo Time-to-Live (TTL) no cabeçalho IP, que evita loops infinitos na rede ao descartar pacotes que excedem o número máximo de saltos permitidos.

1. PROTOCOLOS DA CAMADA DE INTERNET

O protocolo IP (Internet Protocol) é a base da comunicação na Internet, permitindo que dados sejam enviados de um dispositivo para outro. Ele utiliza endereços IP para identificar redes e dispositivos, encapsulando dados em pacotes chamados "datagramas". Esses pacotes são roteados para garantir sua entrega ao destino correto, mesmo em redes complexas compostas por múltiplos roteadores. Entre as versões do protocolo, o IPv4 utiliza endereços de 32 bits, oferecendo cerca de 4,3 bilhões de combinações únicas, mas enfrenta o problema do esgotamento desse espaço devido ao crescente número de dispositivos conectados. O IPv6, por outro lado, utiliza endereços de 128 bits, permitindo um número vastamente maior de endereços disponíveis.

O protocolo ICMP (Internet Control Message Protocol) é utilizado para diagnósticos e relatórios de erro na comunicação de rede. Ele notifica dispositivos sobre problemas, como indisponibilidade de roteadores ou redes, auxiliando na identificação e solução de falhas. Entre as ferramentas que utilizam o ICMP, destacam-se o Ping, que verifica a conectividade entre dispositivos ao medir o tempo de resposta dos pacotes enviados, e o Traceroute, que mapeia o caminho dos pacotes até o destino, permitindo identificar gargalos ou interrupções na rede.

O protocolo ARP (Address Resolution Protocol) é responsável por converter endereços IP (lógicos) em endereços MAC (físicos), essenciais para a entrega de pacotes na camada de enlace em redes locais. Ele mantém uma tabela que associa endereços IP aos respectivos endereços MAC, sendo consultada durante a transmissão de dados. Quando um dispositivo precisa enviar dados a outro na mesma rede, mas não conhece o endereço MAC correspondente, realiza uma solicitação ARP. O dispositivo de destino responde com seu endereço MAC, que é então armazenado no cache ARP para facilitar comunicações futuras.

Enquanto o ARP realiza a conversão de IP para MAC, o protocolo RARP (Reverse Address Resolution Protocol) executa a operação inversa, mapeando endereços MAC para endereços IP. Isso é particularmente útil para dispositivos que não conhecem seu próprio endereço IP ao inicializar, como terminais sem disco. Apesar de sua utilidade em redes locais para configuração automática de dispositivos, o RARP foi amplamente substituído por protocolos mais modernos e robustos, como o DHCP.

1. FUNCIONAMENTO DO ENDEREÇAMENTO IP

O endereçamento IP é um sistema que permite a identificação exclusiva de dispositivos em uma rede, garantindo a comunicação eficiente entre eles. Um endereço IP é um número atribuído a cada dispositivo conectado à rede, possibilitando o envio e recebimento de dados de maneira precisa. Existem duas versões principais: o IPv4, com endereços de 32 bits organizados em quatro números separados por pontos (como 192.168.0.1), e o IPv6, que utiliza 128 bits e é representado por números em formato hexadecimal (como 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Cada endereço IP é dividido em duas partes: o ID de Rede, que identifica a rede a que o dispositivo pertence, e o ID de Host, que especifica o dispositivo dentro da rede.

No IPv4, os endereços são classificados em cinco categorias: A, B, C, D e E, cada uma com uma finalidade específica. A classe A abrange endereços de 0.0.0.0 a 127.255.255.255 e é destinada a redes muito grandes, como provedores de internet, utilizando a máscara padrão 255.0.0.0. A classe B, que cobre endereços de 128.0.0.0 a 191.255.255.255, é usada por organizações de porte médio, como universidades, com a máscara 255.255.0.0. Já a classe C, que inclui endereços de 192.0.0.0 a 223.255.255.255, é ideal para redes pequenas, como residências ou pequenos negócios, e utiliza a máscara 255.255.255.0. A classe D é reservada para multicast, enquanto a classe E é destinada a usos experimentais e futuros.

A máscara de sub-rede desempenha um papel importante no endereçamento IP, dividindo um endereço em partes que identificam a rede e o host. Por exemplo, a máscara 255.255.255.0 indica que os primeiros três octetos são dedicados à rede, enquanto o último define os dispositivos dentro dela. Essa segmentação otimiza o uso de endereços IP, permitindo que grandes redes sejam subdivididas em sub-redes menores. Isso melhora a eficiência do roteamento de dados, facilita a gestão da rede e aumenta a segurança ao isolar segmentos específicos.

A fragmentação de pacotes ocorre na camada de Internet do modelo TCP/IP quando um datagrama IP (pacote de dados) é maior do que o tamanho máximo permitido para transmissão por um determinado enlace. Esse limite é definido pelo MTU (Maximum Transmission Unit). Cada enlace de rede pode ter um MTU diferente, e, quando o tamanho do datagrama excede esse limite, ele é dividido em fragmentos menores para que possa ser transmitido corretamente.

Quando um roteador detecta que o tamanho de um datagrama IP é maior do que o MTU do próximo enlace, ele realiza a divisão do datagrama em partes menores. Cada fragmento contém um cabeçalho IP, que fornece informações essenciais, como o número de identificação do datagrama original, o deslocamento do fragmento em relação ao início do datagrama e um bit que indica se aquele é o último fragmento ou se há mais fragmentos a seguir. Esse processo garante que o datagrama seja dividido de forma que a rede consiga manipulá-lo adequadamente, independentemente das limitações do enlace de rede.

A reconstituição dos fragmentos ocorre no dispositivo de destino. No destino, os fragmentos são reorganizados com base em seus deslocamentos e números de identificação. No entanto, se algum fragmento for perdido ou danificado durante a transmissão, o datagrama inteiro será descartado. Em casos como esse, uma retransmissão pode ser solicitada, dependendo do protocolo de transporte em uso (como o TCP).

1. IMPACTOS NO DESEMPENHO DA REDE

A fragmentação pode gerar impactos no desempenho da rede. Um dos principais problemas é o aumento de sobrecarga. Cada fragmento carrega seu próprio cabeçalho IP, o que aumenta o uso de largura de banda para a transmissão de dados. Esse aumento no consumo de recursos pode afetar a eficiência geral da rede, principalmente em redes com alta quantidade de fragmentos.

Um impacto que podemos citar da fragmentação é a maior complexidade na reconstituição. A necessidade de reorganizar fragmentos no destino pode sobrecarregar os dispositivos finais e causar atrasos na entrega dos dados. Além disso, a perda de dados é uma preocupação importante. Se um fragmento for perdido, o datagrama não poderá ser montado corretamente, resultando na necessidade de retransmissões, o que gera ainda mais tráfego na rede.

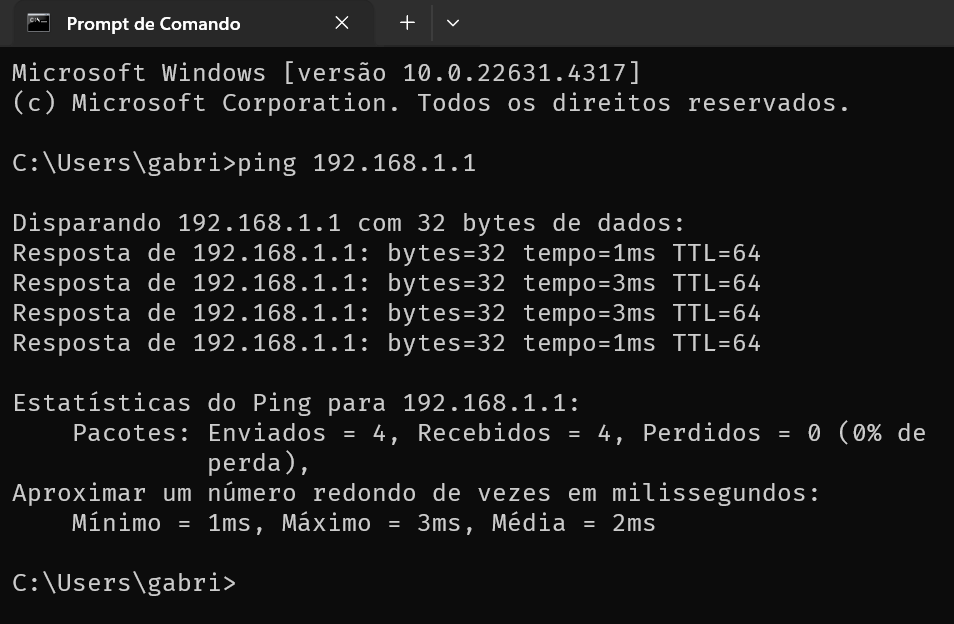
1. SEGURANÇA NA CAMADA DE INTERNET

Na camada de Internet há diversas vulnerabilidades que podem ser exploradas por atacantes. Um exemplo é o spoofing de IP, em que um atacante falsifica o endereço IP de origem de um pacote para mascarar sua identidade. Isso permite que o atacante evite ser rastreado e, muitas vezes, execute outros tipos de ataques, como o Man-in-the-Middle, no qual a comunicação entre duas partes é interceptada e manipulada. Além disso, os ataques de roteamento malicioso podem ser empregados para manipular as tabelas de roteamento, redirecionando o tráfego para destinos não autorizados, o que prejudica a entrega correta dos dados.

Outro risco comum é o ataque de DoS (Negação de Serviço), que visa sobrecarregar a rede com tráfego excessivo, tornando sistemas ou serviços inacessíveis para os usuários legítimos. No caso da fragmentação IP maliciosa, um atacante pode manipular os pacotes IP durante o processo de fragmentação, interferindo na entrega dos dados e podendo causar falhas na comunicação entre dispositivos.

Para mitigar essas ameaças, é essencial adotar medidas de segurança eficazes. O uso de filtros de pacotes e firewalls é uma das estratégias principais. Esses dispositivos de segurança ajudam a bloquear o tráfego malicioso, inspecionando pacotes com base em parâmetros como endereços IP, portas e protocolos, e podem impedir, por exemplo, pacotes IP falsificados ou tráfego originado de fontes suspeitas. Além disso, o uso de VPNs e criptografia para proteger a comunicação de dados, criando uma camada extra de segurança, dificulta a interceptação e a manipulação de dados em trânsito.

1. EXEMPLOS PRATICOS
2. PING

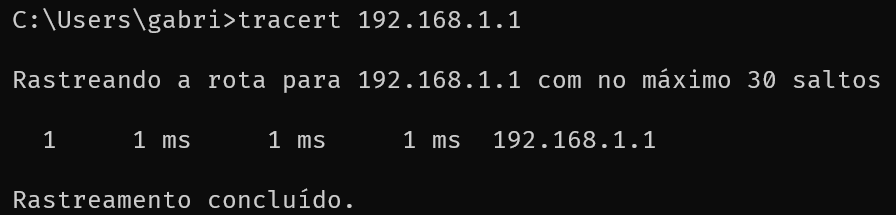


No exemplo acima, foi realizado o teste com o IP 192.168.1.1, o comando enviou 4 pacotes de dados. Todos os pacotes foram recebidos de volta sem perda, o que indica que a comunicação entre os dispositivos foi bem-sucedida.

Além disso, o tempo de resposta variou entre 1ms e 3ms, com uma média de 2ms. Isso indica uma conexão rápida e de baixa latência, comum em redes locais. O valor TTL (Time to Live) foi 64, o que significa que os pacotes passaram por até 64 roteadores na rede antes de serem descartados. O TTL é importante para evitar loops de roteamento, controlando o número de saltos que um pacote pode realizar.

O comando ping tem sua importância para diagnosticar problemas de conectividade. Ele permite verificar se um dispositivo está acessível na rede, medir o tempo de resposta e detectar problemas de latência. Caso haja perda de pacotes, isso pode indicar congestionamento ou falhas no dispositivo de destino ou na infraestrutura da rede.

1. TRACERT



Neste exemplo, o comando tracert foi executado com sucesso, e o resultado mostra que o pacote chegou diretamente ao destino, 192.168.1.1, em apenas 1ms, sem passar por outros saltos intermediários.

Isso indica que o dispositivo de destino (geralmente um roteador ou gateway) está muito próximo da sua máquina, possivelmente na mesma rede local. Ou seja, não há roteadores intermediários entre sua máquina e o destino, o que é típico em redes locais sem a necessidade de comunicação através de vários dispositivos de rede.

Esse comportamento é esperado quando você está fazendo um teste de conectividade com um dispositivo que está na mesma sub-rede ou rede local. Nesse caso, o tempo de resposta foi mínimo, e não houve problemas de roteamento ou latência.

Se o dispositivo de destino estivesse em uma rede diferente (por exemplo, um servidor na internet), o comando tracert mostraria vários saltos até chegar ao destino, cada um representando um roteador ou servidor de rede pelo qual o pacote passou.

REFERENCIAS

ESTRATÉGIA CONCURSOS. Redes de computadores e protocolos de rede. Disponível em: <https://www.estrategiaconcursos.com.br/blog/redes-computadores-protocolos-rede/>. Acesso em: 24 nov. 2024.

CRIANDO BITS. Protocolos da camada de inter-rede. Disponível em: <https://www.criandobits.com.br/protocolos-da-camada-de-inter-rede/>. Acesso em: 24 nov. 2024.

ACÁCIO, A. CCNA - Capítulo 9: Protocolos e serviços da camada de rede. Disponível em: <http://lsi.usp.br/~acacio/CCNA_Cap09Mod01.pdf>. Acesso em: 24 nov. 2024.

DLTEC. Guia definitivo para entender o protocolo TCP/IP. Disponível em: <http://www.dltec.com.br/blog/redes/guia-definitivo-para-o-entender-o-protocolo-tcp-ip/>. Acesso em: 24 nov. 2024.

KINSTA. O que é ARP?. Disponível em: <https://kinsta.com/pt/base-de-conhecimento/o-que-e-arp/>. Acesso em: 24 nov. 2024.

COMPUGRAF. Quais as principais vulnerabilidades de uma rede e como se prevenir. Disponível em: <https://www.compugraf.com.br/blog/quais-as-principais-vulnerabilidades-de-uma-rede-e-como-se-prevenir/>. Acesso em: 26 nov. 2024.

FURG. Protocolos vulneráveis. Disponível em: <https://segurancadainformacao.furg.br/monitoramento/protocolos-vulneraveis>. Acesso em: 26 nov. 2024.

GOCACHE. O que é o modelo OSI, seus ataques e como se proteger. Disponível em: <https://gocache.com.br/seguranca/o-que-e-modelo-osi-seus-ataques-e-como-se-proteger/>. Acesso em: 26 nov. 2024.

AZION. O que é segurança de rede. Disponível em: <https://www.azion.com/pt-br/learning/network-layer/o-que-e-seguranca-de-rede/>. Acesso em: 26 nov. 2024.